UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/743,323 | 12/23/2003 | Dominique Louis Joseph Fedronic | L741.03112 | 5563 |

24257 7590 01/23/2007

STEVENS DAVIS MILLER & MOSHER, LLP
1615 L STREET, NW
SUITE 850
WASHINGTON, DC 20036

| EXAMINER | |
|---|---|
| LE, CANH | |
| ART UNIT | PAPER NUMBER |
| 2109 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 01/23/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/743,323 | FEDRONIC ET AL. | |
| | Examiner | Art Unit | |
| | Canh Le | 2112 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *23 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) *7-8,22,27, 30-31* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12/23/2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/5/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Specification*

The disclosure is objected to because of the following informalities: On page 11, lines 18-19, a CSP2 245t does not match with a label with figure 2. On page 13, line 14 and line 26, a Ks[ID] 205t and a CSP2 245t and do not match with label in figure 2B.

Appropriate correction is required.

### *Claim Objections*

Claims 7- 8, 22, 27, and 30-31 are objected to because of the following informalities:

An abbreviation should spell out the expression the first time it is used and then be followed by parentheses (example, Application Protocol Data unit (APDU)).

For example,

a. In claims 7 and 22, "APDU" should be "Application Protocol Data unit (APDU)"

b. In claims 8 and 27, "SSL, IPsec or TLS" should be " Secure socket layer (SSL), transport layer security (TLS) or internet protocol security (IPsec) "

c. Claims 30 and 31 should depend on claim 29 because they are drawn to a computer program product.

Appropriate correction is required.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

Claims 11, 13, 16-18, 29, and 30-31 are rejected under 35 U.S.C. 102(e) as being anticipated by Band (Publication No.: US 2004/0103324 A1).

***Claim 11***

Band discloses a server mediated security token access system comprising:

a security token enabled client in processing communications with an authentication server and an operatively coupled security token (Figure 1; box 10 (client), box 100 (server), box 5 (security token) ) wherein said security token enabled client includes means for;

receiving a first critical security parameter from a use (Paragraph [0012], lines 9-10) ,

exchanging a plurality of critical security parameters between said security token and said authentication server, wherein said first critical security parameter is a member of said plurality of critical security parameters (Figure 3, Paragraph [0012], lines 10-15; credentials are equivalent to a critical security parameters),

generating an access request which incorporates a unique identifier associated with said security token ( Abstract lines 1-3; Paragraph [0036], lines 4-5),

sending an access request and at least one member of said plurality of critical security parameters to said authentication server (Paragraph [0014], lines 1-5), and said authentication server including means for;

authenticating said user via at least said at least one member,

obtaining a second critical security parameter having an association with said security token, wherein said second critical security parameter is also a member of said plurality of critical security parameters (Paragraph [0014]; a password is a second critical security parameter), and

sending said second critical security parameter to said security token (Paragraph [0014]);

said security token including means for;

authenticating said second critical security parameter (Paragraph [0015]) , and

allowing access to one or more security token resources following successful authentication of said second critical security parameter (Paragraph [0032], lines 3-5).

***Claim 13***

Band also discloses the system according to claim 11 wherein said processing communications includes SSL, IPsec or TLS (Paragraph [0016] and [0028]).

***Claim 16***

Band also discloses the system according to claim 11 wherein said plurality of critical security parameters is selected from the group consisting of a passphrase, a

cryptographic key, biometric data, a password, a security state associated with a security policy and a result of a cryptographic operation (Paragraph [0014]; A password is a critical security parameter).

***Claim 17***

Band also discloses the system according to claim 11 wherein said authentication server further includes means for;

processing a biometric sample sent from said security token enabled client as said first critical security parameter (paragraph [0014], lines 1-5),

generating a sample biometric template (paragraph [0030], lines 13-15),

matching said sample biometric template against a reference biometric template (paragraph [0030], lines 13-15) and returning a cryptographic result to said security token (paragraph [0036], lines 4-8; figure 3, box 5) as said second critical security parameter,

sending said sample biometric template to said security token as said second critical security parameter.

***Claim 18***

Band also discloses the system according to claim 11 wherein said authentication server further includes means for resetting an invalid entry counter associated with said security token following authentication of said second critical security parameter

(paragraph [0026], lines 11-12).

***Claim 29***

Band discloses a computer program product embodied in a tangible form readable by a plurality of processors in processing communications, wherein said computer program product includes executable instructions stored thereon for causing one or more of said plurality of processors to;

a. exchange a plurality of critical security parameters between a first processor , a second processor and a third processor (Figure 3, Paragraph [0012], lines 10-15; credentials are equivalent to a critical security parameters; first processor is in box 10, second processor is box 100; third processor is in box 5),

b. authenticate a first member of said plurality of critical security parameters received by said second processor (Paragraph [0013], lines 1-5; challenge/response are critical security parameters),

c. send a second member of said plurality of critical security parameters to said third processor following authentication of said first member of said plurality of critical security parameters by said second processor (Paragraph [0014]),

d. authenticate said second member of said plurality of critical security parameters by said third processor (Paragraph [0015]), and

e. allow access to a memory coupled to said third processor following successful authentication of said second member of said plurality of critical security parameters

(Paragraph [0032], lines 3-5).

***Claim 30***

Band discloses the computer program product according to claim 28 wherein said tangible form includes magnetic media, optical media or logical media (Figure 3, box 35).

***Claim 31***

Band discloses the computer program product according to claim 28 wherein said executable instructions are stored in a code format selected from the group consisting of compiled, interpreted, compilable and interpretable (Paragraph [0009], line-5).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-5, 8-10, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Band (Publication No.: US 2004/0103324 A1) in view of Le Saint '152 (Publication No.: US 2004/0123152 A1).

***Claim 1***

Band discloses a server mediated security token access method comprising the steps of:

a. exchanging one or more critical security parameters between a security token enabled client, a security token operatively coupled to said security token enabled client and an authentication server (Figure 3, Paragraph [0012], lines 10-15; credentials are equivalent to a critical security parameters).

b. performing a plurality of authentication transactions between at least said security token and said authentication server using said one or more critical security parameters (Paragraph [0013], lines 1-5; challenge/response are critical security parameters) , and

c. allowing said user access to one or more security token resources following successful completion of said plurality of authentication transactions (Paragraph [0037], lines 11-13).

Band does not disclose that a security token is generally unavailable to a user due to implementation of a security policy or a processing limitation.

Le Saint '152 discloses that a security token is generally unavailable to a user due to implementation of a security policy or a processing limitation (Paragraph [0058], lines 1-4). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the method of Band by including requiring implementation of some type of security policies before performing a request transaction of Le Saint '152 because it would provide a consistent and uniform interface to critical security token service such as authentication and secure messaging.

***Claim 2***

Band also discloses the method according to claim 1 wherein step 1.a further includes the steps of;

a. generating by either said security token or said security token enabled client, an access request which incorporates a unique identifier associated with said security token (Paragraph [0014], lines 1-5),

b. sending said access request to said authentication server (Paragraph [0014], lines 1-5), and

c. obtaining a critical security parameter associated with said unique identifier, wherein said critical security parameter is a member of said one or more critical security parameters (Paragraph [0014], lines 1-7; Password is a critical security parameter).

***Claim 3***

Band also discloses the method according to claim 1 wherein said one or more critical security parameters is selected from the group consisting of a passphrase, a cryptographic key, biometric data, a password, a security state associated with said security policy and a result of a cryptographic operation (Paragraph [0014], lines 1-7; Password is a critical security parameter).

***Claim 4***

Band also discloses the method according to claim 1 further including the step of establishing a secure messaging session between said authentication server and at least said security token (Paragraph [0016]).

***Claim 5***

Band also discloses the method according to claim 1 further including the step of resetting an invalid entry counter associated with said security token following successful completion of said plurality of authentication transactions (Paragraph [0026], lines 9-13).

***Claim 8***

Band also discloses the method according to claim 4 wherein said secure messaging session includes SSL, IPsec or TLS (Paragraph [0016] and [0028]).

***Claim 9***

Band also discloses the method according to claim 3 wherein said biometric data is sent from said security token enabled client to said authentication server, processed by said authentication server and returned to said security token as a member of said one or more critical security parameters (Paragraph [0014], lines 1-7; password is a critical security parameter).

***Claim 10***

Band also discloses the method according to claim 3 wherein said biometric data is sent from said security token enabled client to said authentication server, processed by said authentication server, matched against a reference biometric template and a cryptographic result returned to said security token as a member of said one or more critical security parameters (Paragraph [0013], lines 5-10; password is a critical security parameter).

*Claim 19*

Band discloses the system as in claim 11.

Band does not disclose a system of a security token that is generally unavailable to said user due to implementation of a security policy or a processing limitation.

Le Saint '152 discloses the system of a said security token that is generally unavailable to said user due to implementation of a security policy or a processing limitation (Paragraph [0058], lines 1-4). Thus, it would have been obvious to the person of

ordinary skill in the art at the time of the invention was made to modify the system of Band by including requiring implementation of some type of security policies before performing a request transaction of Le Saint '152 because it would provide a consistent and uniform interface to critical security token service such as authentication and secure messaging.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Band (Publication No.: US 2004/0103324 A1) and Le Saint '152 (Publication No.: US 2004/0123152 A1) in view of Le Saint '762 (Publication No.: US 2004/0218762 A1).

***Claim 6***

Band and Le Saint '152 disclose the method as in claim 4.

Band and Le Saint '152 do not disclose a method of a secure messaging session that incorporates a set of session keys generated by said authentication server and shared with said security token.

Le Saint '762 discloses the method of a secure messaging session that incorporates a set of session keys generated by said authentication server and shared with said security token (Paragraph [0011] and [0012]). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the method of Band and Le Saint '152 by including of a set of session keys of Le Saint '762 because it would prevent unauthorized access to the information being exchanged in the secure messaging session.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Band (Publication No.: US 2004/0103324 A1), Le Saint '152 (Publication No.: US 2004/0123152 A1) and Le Saint '762 (Publication No.: US 2004/0218762 A1) in view of Audebert et al. (Publication No.: US 2002/0162021 A1).

***Claim 7***

Band, Le Saint '152, and Le Saint '762 disclose the method as in claim 6 described above.

Band, Le Saint '152, and Le Saint '762 do not disclose a method of a secure messaging session that incorporates an APDU communications pipe.

Audebert discloses the method of a secure messaging session that incorporates an APDU communications pipe (Paragraph [0009] and [0011]). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the method of Band, Le Saint '152, and Le Saint '762 by including of an APDU communication pipe of Audebert because it would provide an overall data processing system that is much easier to maintain and significantly less susceptible to unauthorized access or compromise.

Claims 12, and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Band (Publication No.: US 2004/0103324 A1) in view of Le Saint '762 (Publication No.: US 2004/0218762 A1).

***Claim 12***

Band discloses the system as in claim 11.

Band does not disclose a system of authentication server that further includes means for generating and sharing a set of session keys with said security token.

Le Saint '762 discloses the system of authentication server further that includes means for generating and sharing a set of session keys with said security token (Paragraph [0011], [0012], and [0055]; A cryptographic module is a security token). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the system of Band by including generating and sharing a set of session keys with said security token of Le Saint '762 because it would prevent unauthorized access to the information being exchanged in the secure messaging session.

***Claim 14***

Band further discloses the system according to claim 12 wherein said authentication server and said security token further includes means for establishing a secure messaging session between said authentication server and said security token using said set of session keys (Paragraph [0016]).

***Claim 15***

Le Saint '762 further discloses the system according to claim 12 wherein said security token further includes means for generating and assigning session identifiers to said set of session keys (Paragraph [0011] and [0012]).

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Band (Publication No.: US 2004/0103324 A1) in view of Le Saint '174 (Publication No.: US 2004/0221174 A1).

***Claim 20***

Band discloses the system as in claim 16.

Band does not disclose a system of a security policy that is associated with at least said security token, said security token enabled computer system or said authentication server.

Le Saint '174 discloses the system of a security policy is associated with at least said security token, said security token enabled computer system or said authentication server (Paragraph [0028]; figure 1A, box 152). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the system of Band by including of a security policy is associated with security token of Le Saint '174 because it would provides a consistent and uniform interface to critical security token service such as authentication and secure messaging.

Claims 21, and 22- 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Band (Publication No.: US 2004/0103324 A1) and Le Saint '762 (Publication No.: US 2004/0218762 A1) in view of Le Saint '152 (Publication No.: US 2004/0123152 A1)

***Claim 21***

Band discloses a server mediated security token access system comprising:

a security token enabled client in processing communications with an authentication server and an operatively coupled security token including (Figure 3);

a user input means (box 30);

a first processor (box 10);

a first memory (box 10 and box 35) operatively coupled to said first processor;

a client application (box 15) operatively stored in at least a portion of said first memory having logical instructions executable by said first processor to;

receive a first critical security parameter from said user input means (box 30),

exchange a plurality of critical security parameters between said security token and said authentication server (Figure 3, Paragraph [0012], lines 10-15; credentials are equivalent to critical security parameters), wherein said first critical security parameter is a member of said plurality of critical security parameters ,

generate an access request which incorporates a unique identifier associated with said security token, and send said access request to said authentication server (Paragraph [0014], lines 1-5 ; A user request and performs the functions);

said authentication server including (Figure 1);

a second processor (box 100);

a second memory (box 100 and box 135) operatively coupled to said second processor;

a server application (box 115) operatively stored in at least a portion of said second memory having logical instructions executable by said second processor to;

authenticate a user via said first critical security parameter (Paragraph [0012], lines 1-5),

obtain a second critical security parameter associated with said security token via said unique identifier, wherein said second critical security parameter is also a member of said plurality of critical security parameters (Paragraph [0014]; a password is a second critical security parameter).

Band does not disclose

sending said second critical security parameter to said security token; and

said security token including;

a third processor;

a third memory operatively coupled to said third processor;

a security executive application operatively stored in at least a portion of said third memory having logical instructions executable by said third processor to ;

authenticate said second critical security parameter, and

allow access to one or more security token resources following successful authentication of said second critical security parameter.

Le Saint '762 discloses

sending said second critical security parameter to said security token; and said security token (Figure 1, box 75; A security token includes a cryptographic module) including;

a third processor (Paragraph [0016], lines 1-5; A cryptographic module includes a security executive application which includes the functional capabilities of performing its portion of a secure key exchange) ;

a third memory (Paragraph [0016], lines 1-5) operatively coupled to said third processor;

a security executive application (Figure 1A, box 115; Paragraph [0044]) operatively stored in at least a portion of said third memory having logical instructions executable by said third processor to ;

authenticate said second critical security parameter, and

allow access to one or more security token resources following successful authentication of said second critical security parameter (Paragraph [0052]; lines 1-5).

Band and Le Saint '762 do not disclose a system wherein a security token is generally unavailable to said user due to implementation of a security policy or a processing limitation.

Le saint '152 discloses the system wherein said security token is generally unavailable to said user due to implementation of a security policy or a processing limitation (Paragraph [0058], lines 1-4). Thus, it would have been obvious to the person of ordinary skill in the art at the time of the invention was made to modify the system of

Band and Le Saint '762 by including of a feature security policy of Le saint '152 because it would prevent unauthorized access to the information being exchanged in the secure messaging session and provides a consistent and uniform interface to critical security token service such as authentication and secure messaging.

***Claim 22***

Band, Le Saint '762, and Le Saint '152 disclose the system as in claim 21.

Band, Le Saint '762, and Le Saint '152 do not disclose a system of an authentication server that further includes a pipe server application operatively installed in another portion of said second memory having logical instructions executable by said second processor to;

generate APDU commands,

encapsulate said APDU commands in one or more communications packets, and

extract APDU responses encapsulated in said one or communications packets.

Audebert discloses the system of an authentication server that further includes a pipe server application operatively installed in another portion of said second memory having logical instructions executable by said second processor to;

generate APDU commands,

encapsulate said APDU commands in one or more communications packets, and

extract APDU responses encapsulated in said one or communications packets (Paragraph [0009] and [0011]). Thus, it would have been obvious to the person of

ordinary skill in the art at the time of the invention was made to modify the system of Band, Le Saint '762, and Le Saint '152 by including an APDU communication pipe of Audebert because it would provide an overall data processing system that is much easier to maintain and significantly less susceptible to unauthorized access or compromise.

***Claim 23***

Audebert also discloses the system according to claim 22 wherein said security token enabled client further includes a pipe client application operatively installed in another portion of said first memory having logical instructions executable by said first processor to;

encapsulate said APDU responses in one or more communications packets, and

extract said APDU commands encapsulated in said one or communications packets (Paragraph [0009] and [0011]).

*Claim 24*

Band further discloses the system according to claims 21 wherein said plurality of critical security parameters is selected from the group consisting of a passphrase, a cryptographic key, biometric data, a password, a security state associated with a security policy and a result of a cryptographic operation (Paragraph [0014], lines 1-7; Password is a critical security parameter).

***Claim 25***

Band further discloses the system according to claim 21 wherein said client application further includes logical instructions executable by said first processor to receive a biometric sample from said user (Paragraph [0012], lines 9-10) and send said biometric sample to said authentication server as said first critical security parameter (Paragraph [0029], lines 5-7).

***Claim 26***

Band further discloses the system according to claim 21 wherein said server application authentication further includes logical instructions executable by said second processor to;

process a biometric sample sent from said security token enabled client as said first critical security parameter (paragraph [0014], lines 1-5),

generate a sample biometric template (paragraph [0030], lines 13-15),

match said sample biometric template against a reference biometric template (paragraph [0030], lines 13-15) and return a cryptographic result to said security token (paragraph [0036], lines 4-8; figure 3, box 5) as said second critical security parameter, or

send said sample biometric template to said security token as said second critical security parameter.

***Claim 27***

Band further discloses the system according to claim 21 wherein said processing communications includes SSL, IPsec or TLS (Paragraph [0016] and [0028]).

***Claim 28***

Le Saint '762 further disclose the system according to claim 21 wherein said processing communications includes a set of session keys generated by said authentication server and shared with said security token (Paragraph [0011] and [0012]).

***Conclusion***

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

The DiGiorgio et al. (US Patent: 6,385,729 B1) disclose a secure token device access to services provided by internet service provider (ISP).

The Audebert et al. (Pub. No.: US 2004/0148429 A1) disclose a method and system for remote activation and management of personal security devices.

The O'Donnell at al. (US Patent: 7,024,689 B2) disclose granting access rights to unattended software.

The Pitchenik et al. (US Patent: 6,397,328 B1) disclose a method for verifying the expected postage security device and an authorized host system.

The Vandergeest et al. (Pub. No.: US 2002/0169988 A1) disclose a method and apparatus for providing user authentication using a back channel.

The Pare, Jr. et al. (US Patent: 5,838,812) disclose a tokenless biometric transaction authorization system.

The Shinzaki (US Patent: 6,957,339 B2) discloses a user verification system, and portable electronic device with user verification function utilizing biometric information.

The swift et al. (US Patent: 5,719,941) disclose a method for changing passwords on a remote computer.

The Priebatsch (Pub. No.: US 2004/0103325 A1) discloses an authentication remote pin unblock.

The Bianco at al. (US Patent: 6,256,737 B1) disclose a system, method and computer program product for allowing access to enterprise resources using biometric devices.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Walter Griffin can be reached on 571-272-1447. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
January 10, 2007

WALTER D. GRIFFIN
SUPERVISORY PATENT EXAMINER